PRINCIPLES, CONSTRAINTS, AND ASSUMPTIONS

Department of Transportation

DELPHI Program

Author:	DELPHI Program Team
Creation Date:	May 4, 1998
Last Updated:	5/11/98 12:02 PM
Control Number:	TIR350
Version:	4

Contents

Introduction

Purpose

The purpose of this Principles, Constraints, and Assumptions document is to define the approach to developing and implementing the technical infrastructure necessary to execute and support the DELPHI Program.

Scope

The Principles, Constraints, and Assumptions document describes major technology-related strategies and addresses major management and architectural issues associated with establishing the DELPHI technical infrastructure. The following topics are covered in this plan:

- Considerations, Assumptions and Known Constraints
- Risks and Risk Mitigation Strategies
- Guiding Principles

The responsibility for executing strategies defined within the Principles, Constraints, and Assumptions document resides with the DELPHI Technical Infrastructure Group in close coordination with the DOT Program Management Team.

Related Documents

1. Program Charter for the DELPHI Program
2. SDL Facility Plan for the DELPHI Program
3. Documentation Facility Plan for the DELPHI Program

Considerations, Assumptions and Known Constraints

Considerations

The following items are key considerations for defining and establishing the DELPHI Technical Infrastructure:

- In the event Oracle Federal Financial 2.0 is delayed in its release, a decision is expected to occur in August 1998 with respect to alternatives. A decision to use Oracle Federal Financials 1.1 in lieu of 2.0 may impact configuration of the infrastructure since 1.1 is a client/server design whereas 2.0 is a web-based design.
- The ADTN2000 network will be supported as the primary data communications vehicle for DELPHI access by all Operating Administrations. Alternate mechanisms may also be considered.

Assumptions

Content and context within the Principles, Constraints, and Assumptions document are based on the following assumptions:

- System Requirements and Design documents necessary to implement the technical infrastructure have been developed in advance of the project and will be available for the confirmation and validation process. These documents should address the following areas:
    - ✓ Hardware Architecture
    - ✓ Network Architecture
    - ✓ System Security
    - ✓ System Capacity
    - ✓ Data and Data Conversion Requirements
    - ✓ Telecommunications Architecture
    - ✓ System Performance Requirements
    - ✓ External Systems Connectivity Requirements
    - ✓ Logistical Configuration (e.g. database replication for remote sites)
    - ✓ Redundancy and Fault Tolerance Requirements
- Human resources to execute the plan will be available in a timely manner.
- Computing resources and facilities will be available within the scheduled project time frames.
- Equipment procurement processes will not experience delays.
- Connectivity to external systems will be nonexistent or greatly limited.

Known Constraints

The following are known constraints associated with establishing the DELPHI Technical Infrastructure:

- Procurement process for leasing major equipment normally takes 120 calendar days. (See “Impact of Equipment Procurement Process on DELPHI Program Timing” under section “Risks and Risk Mitigation Strategies.”)

- The interim infrastructure to support the Solution Demonstration Lab (SDL) process, etc. will rely on existing equipment (dual DEC Alpha 2100) to function as temporary servers. These servers and related storage devices currently serve other DOT functions and are only available during a specified window of time (i.e. several months). If there is a delay in acquiring the initial DELPHI production server (DEC Alpha 8400), there will be a need to extend the use of temporary servers.

Risks and Risk Mitigation Strategies

The Technical Infrastructure project has inherent risks. Those risks are identified below along with mitigation strategies to minimize the impact of those risks upon the project.

Impact of Equipment Procurement Process on DELPHI Program Timing

The procurement process for leasing major equipment (i.e. the primary servers) requires 90-120 calendar days. Unmanaged, delays in equipment acquisition will affect the ability to execute other related DELPHI projects and activities (e.g. SDL process) in a timely manner. Furthermore, leasing will depend on year-to-year fiscal funding.

In order to facilitate timely deployment of the SDL Facility the following equipment acquisition strategy is prescribed:

- Utilize existing servers (i.e. DEC Alpha 2100 computers) as an interim environment to facilitate the initial 6-months of the SDL process. The existing server computers allow for early deployment of an interim SDL environment and should suffice for the anticipated number of initial users (approximately 50-150 persons; 50 simultaneous).
- Advanced acquisition of one of the anticipated deployed server (i.e. DEC Alpha 8400 computer) will be required in order to facilitate the second phase of SDL processes. (See separate risk assessments below.) This will enable the execution of SDL for the anticipated higher volume of computing activities during the second phase and allow for testing of functionality/response on the actual deployed equipment.
- Leasing agreement should state that lease will be based on available fiscal funding and that no penalty will ensue in the event funding becomes temporarily unavailable.

Acquisition of Equipment Prior to Validating Performance and Suitability

In ideal circumstances, equipment is acquired only after the system design is validated and only after thorough performance testing combined with a validated evaluation of the equipment's suitability. Because of existing program timing constraints, server equipment (at least one machine) must be acquired before the system design is validated and before the machine is actually tested for performance, capability and capacity.

To mitigate the risk of acquiring the wrong machine or size of machine, the following strategy is prescribed:

- Establish an option within the leasing agreement to 1) allow equipment reconfiguration, and 2) allow for early lease termination if the planned equipment assessment determines that the vendor's equipment is significantly flawed for its intended purpose or is otherwise not suitable for the project (e.g. poor actual performance.)

Longevity of Server Equipment Product Line

It is uncertain whether the existing server computing platforms sold by the vendor will remain supported in the near future. To mitigate this uncertainty, the following actions are prescribed:

- Establish contractual obligations with the vendor (as part of the residual purchase component of the lease agreement) to supply additional 100%-compatible processors at a predetermined threshold/"not to exceed" price and for a predetermined period of time. Furthermore, we shall establish contractual obligations with the vendor to provide parts and accessories for a predetermined period of time. We shall retain the right to acquire similarly available processors and parts from third parties at competitive prices.
- Establish contractual obligations with the vendor for a free upgrade/exchange of our equipment with equipment of similar capability should the equipment become designated/announced for sunset (retired) within one-year from date of equipment receipt. Furthermore, if equipment of similar or greater capability is unavailable from the vendor or such equipment is not suitable to task, the vendor shall allow for early termination of the lease.

Dependency on ADTN2000 and DOT IDN for Data Communications

The planned DELPHI infrastructure depends on the ADTN2000 network and DOT IDN to support bandwidth requirements for operating Oracle web-based Federal Financials applications. Since bandwidth requirements for DELPHI's web-based applications can vary substantially depending on actual system utilization, it is possible that the combined load of DELPHI and other DOT systems will exceed ADTN2000 and DOT IDN network capacity--resulting in poor system performance for all users of the network.

To minimize the risk of insufficient network capacity, the following strategy is prescribed:

- Forecast bandwidth needs as early as possible to allow the ADTN2000 and DOT IDN organization to adjust capacity in a timely manner.
- Partner with the ADTN2000 and DOT IDN organization to identify requirements as soon as possible and work with them on an ongoing basis.
- Develop a DELPHI communication plan that maintains involvement and commitment from ADTN2000 and DOT IDN management and support personnel.
- Prepare contingency plans (e.g. use of alternate communications providers; use of supplemental/multiple communications channels; use of de-centralized server architecture).

Guiding Principles

The following principles are intended to serve as guidelines for decision making by the technical team and help ensure consistent application of technology.

Guiding Principles

Principle	Rationale	Implications	Models	Specifications
We will employ commercially available products whenever possible.	The use of commercial off-the-shelf (COTS) products allows DOT to take advantage of industry best practices, competitive pricing and timely updates.	The new systems will displace the old systems.		
We will not customize nor use custom-made products.	Customized products increases the cost and level of effort needed to deploy vendor-supplied updates to products.	We will have access to new functionality and may need to adjust the way we do things today.		
We will favor products that conform to open systems and industry standards.	Using products that are open and based on industry standards enhances the product's longevity and likelihood of connectivity to other products.	Standards typically translate to competition, lower pricing, and better interconnectivity, but may sometimes mean higher up-front cost.	• ISO • CCITT • IEEE • ISA • OSF	• Cisco Routers
We will employ industry best practices.	We can maximize our productivity while reducing our risk exposure by leveraging the experience of others and through their lessons learned.	We will benefit from best practices and may need to change the way we currently operate in order to adopt them.		
We will use standard network protocols based primarily on open standards.	We can capitalize on the critical mass already obtained with internet-based technologies (e.g. browsers, development frameworks, languages). Utilizing these technically mature open technologies should reduce our implementation and support costs.	Many standards capitalize on existing technology while others will require retiring existing products.		• TCP/IP will be our standard protocol for both LANs and WANs • We will use internet protocols like HTML, FTP, SMTP, SNMP
We will establish a technology foundation that supports accessibility to common data across the enterprise.	A central data repository allows for better access and analysis of data captured throughout the system(s). Besides providing a single point for data retrieval, this centralization will better facilitate system backup processes and helps maximize benefits from economies of scale.	We must undertake appropriate data modeling and cataloging so that users can locate the data that they need. We may need to perform tactical data clean up activities to ensure the delivery of high quality data.	• Data warehouses and data marts • Data Quality • Integrated data architecture • Knowledge management	
We will have data security mechanisms commensurate with risk and will comply with established government security requirements.	Technology changes translate to more opportunity for security breach. We must carefully evaluate the technologies deployed in our environment to ensure that security risks are addressed.	Most security risk associated with new technology can be mitigated through changes in management and operating procedures.	• anti-virus software • firewalls	• SSL (secure sockets layer) compatible web servers • RACF on mainframe where applicable

Principle	Rationale	Implications	Models	Specifications
We will provide systematic backup and recovery provisions that ensure protection from unintentional data loss.	In large-scale systems, a single occurrence of data loss that impacts the entire user community can mean many lost hours of productivity and as an aggregate, translates to substantial sums of money.	By ensuring that operating procedures and backup technology are up-to-date, we can reduce the impact of system outage	• redundancy • fault tolerant systems • archive storage • disaster recovery • scheduled network backups	• optical disk archive • tape library robotics
We will balance the need for flexible systems with the need for economic rationalization combined with strategic value.	It is very desirable to have systems that adapt to the way we do business and that can change as our business changes. Regardless of the system need, we must consider alternatives that may include non-technology-oriented solutions and solutions that are temporary.	Sometimes, the best decision includes extending the life of a current system or acquiring a temporary system.		
We will minimize the number of supported desktop and server configurations and will standardize around one or two platforms.	Multiple types of systems require multiple skill sets and multiple configurations that must be diagnosed. We can minimize support costs and increase the effectiveness of our support efforts by minimizing the number of types of systems and operating environments that must be supported.	Having fewer systems to support will increase our effectiveness and efficiency while reducing the ability for support custom solutions.		
We will ensure that the infrastructure supports a layered approach to systems development and deployment (e.g. 3-tiered architecture).	We need to make sure that systems are segmented so that changes at each layer of the infrastructure do not require a major retrofit of other components (e.g. changing the workstation will not require changing the network or servers).	Currently, there are fewer tools designed to support this architecture type than more established ones, but the technology is gaining rapidly.	• Client/Server approach • 3-tiered architecture • N-tiered architecture • Layers with standardized middleware wherever possible • Thick vs. Thin infrastructure	• Forte • Lynx • Gupta • DCOM • DSOM • RPC
We will balance the need for a thick vs. thin infrastructure.	A thick infrastructure will enable deployment of thin-client computing. This typically translates to ease of implementing updates and changes to application programs.	Depending on the current network design & capacity, establishing a thick infrastructure may or may not increase infrastructure development.		